ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

УКАЗАНИЕ

«25» марта 2022 г. № 6103-У

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 69846
от "30" августа 2022 г.

О внесении изменений в Положение Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

На основании статьи 57[1] Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»[1] и части первой статьи 11[1-2] Федерального закона от 2 декабря 1990 года № 395-I «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ)[2]:

1. Внести в Положение Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[3] следующие изменения:

---

[1] Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2013, № 27, ст. 3438; 2019, № 49, ст. 6953.
[2] Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2013, № 27, ст. 3438.
[3] Зарегистрировано Минюстом России 3 июня 2020 года, регистрационный № 58577.

1.1. В пункте 1.4:

абзац двенадцатый изложить в следующей редакции:

«риск нарушения способности кредитной организации (головной кредитной организации банковской группы) поддерживать операционную устойчивость кредитной организации (головной кредитной организации банковской группы), включающую обеспечение непрерывности осуществления критически важных процессов и критически важных операций, определенных кредитной организацией в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения (далее – операционная устойчивость), в результате воздействия источников операционного риска, указанных в пункте 3.3 настоящего Положения, а также изменений процессов кредитной организации (головной кредитной организации банковской группы) или действий третьих лиц, включая нарушения операционной надежности, требования к которой установлены Банком России в соответствии со статьей 57^5 Федерального закона № 86-ФЗ (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 1, ст. 53) (далее соответственно – операционная надежность, риск нарушения непрерывности деятельности).»;

дополнить абзацем следующего содержания:

«В случае если в кредитной организации (головной кредитной организации банковской группы, участнике банковской группы) отсутствуют специализированные подразделения, процедуры управления отдельными видами операционного риска выполняет служба управления рисками.».

1.2. В пункте 2.1:

абзац третий подпункта 2.1.1 после слова «абзацев» дополнить словом «шестого,»;

в подпункте 2.1.4:

в абзаце втором слово «Положения;» заменить словами: «Положения. Кредитная организация (головная кредитная организация банковской группы) применяет агрегированную оценку уровня операционного риска в случае, если кредитная организация (головная кредитная организация

банковской группы) использует методы количественной оценки потерь от реализации операционного риска на основе статистических данных из базы событий с использованием продвинутого подхода, включающего методы, указанные в пункте 4.4 приложения 1 к Указанию Банка России № 3624-У (далее – продвинутый подход);»;

абзац четвертый изложить в следующей редакции:

«оценку ожидаемых потерь от реализации операционного риска в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с использованием статистических данных по событиям операционного риска, зарегистрированным в базе событий в этих разрезах (при наличии), в целях определения способов покрытия указанных ожидаемых потерь, в том числе их учета в ценообразовании услуг и тарифов. Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах методы и порядок проведения оценки ожидаемых потерь от реализации операционного риска.»;

в подпункте 2.1.5:

абзац второй после слова «абзацами» дополнить словом «шестым,»;

абзац четвертый дополнить словами «, в том числе моделирование угроз, включающее анализ потенциальных источников реализации операционного риска и возможных потерь от них (далее – моделирование угроз), с учетом осуществляемых кредитной организацией процессов и форм (способов) контроля операционного риска»;

абзац шестой изложить в следующей редакции:

«Подразделение, ответственное за организацию управления операционным риском, разрабатывает на ежегодной основе план мероприятий по проведению качественной оценки уровня операционного риска с обязательным включением в него перечня критически важных процессов, определенных кредитной организацией (головной кредитной организацией банковской группы) в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения, и перечня процессов, уровень существенности операционного риска у которых по результатам

качественных оценок, предшествующих дате проведения качественной оценки уровня операционного риска, был высоким или очень высоким в соответствии с абзацем одиннадцатым настоящего подпункта или не оценивался в течение двух лет, предшествующих дате проведения качественной оценки уровня операционного риска, в отношении которых осуществляется качественная оценка уровня операционного риска, с указанием ответственных и участвующих подразделений кредитной организации (головной кредитной организации банковской группы) (далее – план проведения качественной оценки). Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) утверждает план проведения качественной оценки.»;

абзац восьмой изложить в следующей редакции:

«Самооценка операционного риска проводится подразделениями кредитной организации (головной кредитной организации банковской группы) в отношении выполняемых ими процессов в соответствии с внутренними документами кредитной организации (головной кредитной организации банковской группы) не реже одного раза в год по установленной во внутренних документах методике (в виде анкетирования выделенных для самооценки операционного риска работников подразделений кредитной организации (головной кредитной организации банковской группы) по направлениям деятельности, в том числе в разрезе составляющих их процессов, которые включены в план проведения качественной оценки, с использованием формализованных анкет).»;

в абзаце одиннадцатом слово «вероятности» заменить словами «количественной и качественной оценки вероятности реализации»;

в абзаце двенадцатом слова «действующих на момент проведения оценки» заменить словами «как действующих на момент проведения оценки, так и рассматриваемых кредитной организацией (головной кредитной организацией банковской группы) к внедрению»;

абзац семнадцатый изложить в следующей редакции:

«Кредитная организация (головная кредитная организация банковской группы) определяет в порядке проведения сценарного анализа операционных рисков критерии проведения сценарного анализа операционных рисков в отношении выявленных операционных рисков в ходе качественной оценки уровня операционного риска, проводимой в соответствии с планом проведения качественной оценки, а также в отношении источников операционного риска, которые не реализовались в деятельности кредитной организации (головной кредитной организации банковской группы), по которым уровень существенности операционного риска оценивается как высокий или очень высокий в соответствии с абзацем одиннадцатым настоящего подпункта.»;

дополнить абзацами следующего содержания:

«Кредитная организация (головная кредитная организация банковской группы) проводит оценку негативного влияния выявленных сценариев реализации операционных рисков и источников операционного риска на свою деятельность в разрезе направлений деятельности и составляющих их процессов с учетом задействованных при их выполнении других процессов и (или) информационных систем, а также с учетом участия третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы) в выполнении процессов кредитной организации (головной кредитной организации банковской группы) (далее – зависимость процессов от третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы).

Кредитная организация (головная кредитная организация банковской группы) в целях проведения качественной оценки видов операционного риска разрабатывает во внутренних документах методику моделирования угроз реализации вида операционного риска и порядок проведения моделирования угроз, в том числе порядок оценки негативного влияния угроз по шкале качественных оценок, разработанной в соответствии с абзацем двенадцатым подпункта 3.13.2 пункта 3.13 настоящего Положения.»;

в абзаце пятом подпункта 2.1.6 слово «совокупных» исключить.

1.3. Подпункт 3.9.9 пункта 3.9 после слова «персоналом» дополнить словами «, корпоративное управление и управление капиталом кредитной организации (головной кредитной организацией банковской группы)».

1.4. Пункт 3.10 дополнить абзацем следующего содержания:

«В случае если кредитной организацией (головной кредитной организацией банковской группы) определено более одного направления деятельности первого уровня в отношении реализовавшегося события операционного риска, кредитная организация (головная кредитная организация банковской группы) указывает в базе событий все направления деятельности первого уровня, в которых реализовалось событие операционного риска, и определяет наиболее значимое направление деятельности первого уровня.».

1.5. В пункте 3.12:

подпункт 3.12.3 изложить в следующей редакции:

«3.12.3. Денежные выплаты клиентам, контрагентам, работникам кредитной организации и другим третьим лицам в целях компенсации им во внесудебном порядке убытков, понесенных ими как в результате действий третьих лиц, так и в результате реализации иных источников операционного риска, в том числе компенсированные кредитной организацией хищения средств клиентов, контрагентов, работников и третьих лиц (с раздельным учетом потерь, которые были компенсированы кредитной организацией, и потерь, которые впоследствии были компенсированы третьими лицами, в том числе страховыми организациями, иностранными страховыми организациями).

Кредитная организация (головная кредитная организация банковской группы) классифицирует вид прямых потерь, указанный в абзаце первом настоящего подпункта, в разрезе работников, а также клиентов, контрагентов и третьих лиц по следующим группам: физические лица, индивидуальные предприниматели, лица, занимающиеся частной практикой, юридические лица.»;

в подпункте 3.12.8 слова «или на» заменить словами «и (или)»;

подпункт 3.12.9 дополнить словами «, в том числе переоценка стоимости активов в сторону уменьшения и (или) исключения из расчета величины собственных средств (капитала) по предписанию Банка России».

1.6. В пункте 3.13:

в подпункте 3.13.2:

абзац третий изложить в следующей редакции:

«нарушение операционной устойчивости кредитной организации (головной кредитной организации банковской группы) в случае, если кредитная организация (головная кредитная организация банковской группы) не определила его в денежном выражении, и (или) приостановку основных и прочих процессов, определяемых кредитной организацией (головной кредитной организацией банковской группы) в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения, в результате события операционного риска, в том числе возникшего в результате сбоев систем и оборудования;»;

абзац двенадцатый изложить в следующей редакции:

«Кредитная организация (головная кредитная организация банковской группы) в отношении каждой качественной потери проводит оценку ее значимости в соответствии с установленной во внутренних документах кредитной организации (головной кредитной организации банковской группы) шкалой качественных оценок потерь по четырехуровневой шкале: «очень высокие», «высокие», «средние», «низкие».»;

подпункт 3.13.3 дополнить абзацем следующего содержания:

«Кредитная организация (головная кредитная организация банковской группы) классифицирует потери, указанные в абзаце втором настоящего подпункта, в разрезе клиентов и контрагентов по следующим группам: физические лица, индивидуальные предприниматели, лица, занимающиеся частной практикой, юридические лица.».

1.7. В пункте 4.1:

в подпункте 4.1.1:

абзац первый после слова «Положения,» дополнить словами «в том числе технологических процессов, требующих обеспечения информационного взаимодействия, обработки и хранения информации с помощью информационных систем (далее – технологические процессы),»;

в абзаце втором слова «процессы, основные, обеспечивающие» заменить словом «, основные»;

абзацы третий и четвертый изложить в следующей редакции:

«К критически важным процессам относятся процессы, которые обеспечивают выполнение операций кредитной организации (головной кредитной организации банковской группы), указанных в пунктах 1–4 и 9 части первой статьи 5 Федерального закона «О банках и банковской деятельности» (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2011, № 27, ст. 3873), ведение бухгалтерского учета, представление отчетности в Банк России в соответствии с Указанием Банка России от 8 октября 2018 года № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации», зарегистрированным Министерством юстиции Российской Федерации 13 декабря 2018 года № 52992, 13 декабря 2019 года № 56796, 18 июня 2020 года № 58705, 30 сентября 2020 года № 60147, 26 марта 2021 года № 62892, 15 апреля 2021 года № 63150, 11 июня 2021 года № 63866, 14 декабря 2021 года № 66316 (далее – Указание Банка России № 4927-У), поддержание ликвидности, выполнение операций на финансовых рынках, кассовых операций, работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций, соблюдение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2021, № 27, ст. 5159), Трудового кодекса Российской Федерации (Собрание законодательства Российской Федерации, 2002, № 1, ст. 3; 2022, № 9, ст. 1259),

Федерального закона «О банках и банковской деятельности» (далее – критически важные операции), а также другие процессы, которые определены кредитной организацией (головной кредитной организацией банковской группы) и прерывание функционирования которых оказывает влияние на выполнение обязательств перед клиентами и контрагентами кредитной организации (головной кредитной организации банковской группы).

К основным процессам относятся процессы, которые обеспечивают выполнение операций, указанных в пунктах 5–7^3 части первой статьи 5 Федерального закона «О банках и банковской деятельности» (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2017, № 31, ст. 4761), в случае если они не отнесены кредитной организацией (головной кредитной организацией банковской группы) к критически важным процессам, а также процессы, которые обеспечивают выполнение операций и услуг, объем которых формирует величину расходов и (или) доходов кредитной организации (головной кредитной организации банковской группы) более 5 процентов от дохода за отчетный год для целей расчета капитала на покрытие операционного риска, определяемого в соответствии с пунктом 3 Положения Банка России от 3 сентября 2018 года № 652-П «О порядке расчета размера операционного риска», зарегистрированного Министерством юстиции Российской Федерации 19 ноября 2018 года № 52705, 19 декабря 2018 года № 53050, 31 марта 2020 года № 57915 (далее – Положение Банка России № 652-П) (далее – доход за год для целей расчета капитала на покрытие операционного риска), в случае если кредитная организация применяет для целей расчета размера операционного риска Положение Банка России № 652-П, или более 5 процентов от величины бизнес-индикатора кредитной организации (головной кредитной организации банковской группы) на последнюю дату ее расчета, которая определяется в соответствии с пунктом 2.2 Положения Банка России от 7 декабря 2020 года № 744-П «О порядке расчета размера

операционного риска («Базель III») и осуществления Банком России надзора за его соблюдением», зарегистрированного Министерством юстиции Российской Федерации 29 января 2021 года № 62290 (далее – Положение Банка России № 744-П), в случае если кредитная организация применяет для целей расчета размера операционного риска Положение Банка России № 744-П. Кредитная организация (головная кредитная организация банковской группы) проводит регулярный (не реже одного раза в год) анализ необходимости пересмотра основных процессов с учетом пункта 4.6 настоящего Положения.»;

в подпункте 4.1.5:

абзац первый дополнить словами «, включая случаи фактической реализации риска нарушения непрерывности деятельности кредитной организации (головной кредитной организации банковской группы), в том числе случаи фактического нарушения требований к операционной надежности (далее – событие риска нарушения непрерывности деятельности)»;

абзац шестой дополнить словами «, включая установление во внутренних документах кредитной организации (головной кредитной организации банковской группы) требований к третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы), обеспечивающим выполнение критически важных процессов и (или) функционирование информационных систем кредитной организации (головной кредитной организации банковской группы), в части системы управления операционным риском третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы), в том числе риском нарушения непрерывности деятельности, и реализации контроля за соблюдением данных требований»;

абзац восьмой дополнить словами «, в том числе мероприятия, разрабатываемые в целях управления риском нарушения непрерывности деятельности»;

в абзаце двенадцатом слова «, в случае реализации операционного риска» заменить словами «и их тестирование в случаях реализации операционного риска, влияющих на непрерывность осуществления критически важных процессов и (или) функционирование информационных систем и предусмотренных сценариями реализации операционного риска, определенными в рамках проведения сценарного анализа в соответствии с подпунктом 2.1.5 пункта 2.1 настоящего Положения»;

абзац пятнадцатый дополнить словами «, в том числе с третьими лицами (внешними подрядчиками, контрагентами, участниками банковской группы)».

1.8. В подпункте 4.2.4 пункта 4.2:

абзацы тринадцатый и четырнадцатый после слов «возмещений по» дополнить словом «прямым»;

в абзаце пятнадцатом слово «(фактических)» исключить.

1.9. Пункт 4.3 дополнить подпунктами 4.3.3 и 4.3.4 следующего содержания:

«4.3.3. Требования к перечню процессов кредитной организации (головной кредитной организации банковской группы), указанному в подпункте 4.1.1 пункта 4.1 настоящего Положения.

Кредитная организация (головная кредитная организации банковской группы) при составлении и ведении перечня процессов кредитной организации (головной кредитной организации банковской группы), указанного в подпункте 4.1.1 пункта 4.1 настоящего Положения, обеспечивает:

выявление и учет взаимосвязей между критически важными процессами, работниками подразделений, информационными системами и информацией, задействованными при выполнении критически важных процессов (далее – взаимосвязи между критически важными процессами), с учетом зависимости процессов от третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы);

мониторинг изменений выявленных взаимосвязей между критически важными процессами.

4.3.4. Требования к управлению операционным риском, возникающим при внесении изменений в критически важные процессы кредитной организации (головной кредитной организации банковской группы) и (или) информационные системы, используемые при выполнении критически важных процессов, включающие соблюдение следующих процедур:

выявление и оценка операционного риска при принятии кредитной организацией (головной кредитной организацией банковской группы) решения об осуществлении функций подразделений кредитной организации (головной кредитной организации банковской группы), банковских операций, услуг, которые кредитная организация (головная кредитная организация банковской группы) не выполняла или не оказывала в течение календарного года, других изменениях, вносимых в критически важные процессы кредитной организации (головной кредитной организации банковской группы), а также оценка влияния выявленного операционного риска на контрольные показатели уровня операционного риска кредитной организации (головной кредитной организации банковской группы), определенные в соответствии с главой 5 настоящего Положения;

оценка влияния изменений, вносимых в процессы, на критически важные процессы кредитной организации (головной кредитной организации банковской группы) с учетом взаимосвязей между критически важными процессами и наличия зависимости процессов от третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы);

организация ресурсного обеспечения (кадрового и финансового), необходимого для осуществления функций подразделений кредитной организации (головной кредитной организации банковской группы), банковских операций, услуг, которые кредитная организация (головная кредитная организация банковской группы) не выполняла или не оказывала в течение календарного года, и других изменений, вносимых в критически

важные процессы кредитной организации (головной кредитной организации банковской группы), до начала их выполнения или оказания кредитной организацией (головной кредитной организации банковской группы);

утверждение решением органа управления кредитной организации функций подразделений кредитной организации (головной кредитной организации банковской группы), банковских операций, услуг, которые кредитная организация (головная кредитная организация банковской группы) не выполняла или не оказывала в течение календарного года, и других изменений, вносимых в критически важные процессы кредитной организации (головной кредитной организации банковской группы), включая функции, операции, услуги, переданные (или частично переданные) на выполнение третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы);

централизованный учет и мониторинг функций подразделений кредитной организации (головной кредитной организации банковской группы), банковских операций, услуг, которые кредитная организация (головная кредитная организация банковской группы) не выполняла или не оказывала в течение календарного года, и других изменений, вносимых в критически важные процессы кредитной организации (головной кредитной организации банковской группы), включая функции, операции, услуги, переданные (или частично переданные) на выполнение третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы), в целях последующей оценки их влияния на контрольные показатели уровня операционного риска кредитной организации (головной кредитной организации банковской группы), определенные в соответствии с главой 5 настоящего Положения;

планирование и контроль внедрения функций подразделений кредитной организации (головной кредитной организации банковской группы), банковских операций, услуг, которые кредитная организация (головная кредитная организация банковской группы) не выполняла или

не оказывала в течение календарного года, и других изменений, вносимых в критически важные процессы кредитной организации (головной кредитной организации банковской группы).».

1.10. В абзаце первом пункта 4.4 слово «указанном» заменить словом «указанным».

1.11. Абзац второй пункта 5.2 изложить в следующей редакции:

«утверждает сигнальные и контрольные значения контрольных показателей уровня операционного риска на плановый годовой период в целом по кредитной организации (головной кредитной организации банковской группы), которые ежегодно подлежат пересмотру и актуализации кредитной организацией (головной кредитной организацией банковской группы) в рамках оценки соответствия процедур управления рисками текущей ситуации в кредитной организации (головной кредитной организации банковской группы), проводимой в соответствии с абзацем первым пункта 3.5 Указания Банка России № 3624-У, в том числе по результатам оценки эффективности функционирования системы управления операционным риском в соответствии с пунктом 4.4 настоящего Положения;».

1.12. Пункт 5.3 дополнить абзацем следующего содержания:

«Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах орган управления кредитной организации (головной кредитной организации банковской группы), который утверждает сигнальные и контрольные значения контрольных показателей уровня операционного риска на плановый годовой период в разрезе направлений деятельности, в том числе составляющих их процессов, и подразделений, ответственных за осуществление операций и сделок и за результаты процесса, с учетом сигнальных и контрольных значений контрольных показателей уровня операционного риска в целом по кредитной организации (головной кредитной организации банковской группы),

утвержденных в соответствии с абзацем вторым пункта 5.2 настоящего Положения.».

1.13. В пункте 6.6:

абзац второй дополнить словами «(группы событий операционного риска)»;

абзац третий дополнить словами «, с указанием количества событий операционного риска в группе»;

абзац восемнадцатый после слова «видами» дополнить словами «операционного риска (риском информационной безопасности, риском нарушения непрерывности деятельности и другими) и другими видами»;

абзац двадцать первый изложить в следующей редакции:

«направления деятельности первого уровня в соответствии с пунктом 3.9 настоящего Положения с указанием наиболее значимого из них;»;

абзац двадцать пятый дополнить словами «, в случае если кредитная организация (головная кредитная организация банковской группы) в соответствии с внутренними документами разрабатывает их при реализации данного события операционного риска»;

абзац двадцать восьмой после слова «валовых» дополнить словом «прямых»;

абзац двадцать девятый после слов «от реализации события операционного риска» дополнить словами «(группы событий операционного риска)»;

в абзаце тридцатом слова «то есть дату отражения» заменить словами «то есть в случае реализации прямой потери – дату отражения прямой», дополнить словами «, в случае реализации непрямой потери – дату регистрации события операционного риска»;

в абзаце тридцать первом слова «(суммы косвенной потери при возможности ее определения)» исключить;

абзацы тридцать четвертый – тридцать шестой изложить в следующей редакции:

«агрегированную сумму валовых прямых потерь и сумму косвенных потерь в рублях накопленным итогом с даты регистрации первой потери;

агрегированную сумму валовых прямых потерь в рублях накопленным итогом с даты регистрации первой потери;

сумму косвенных потерь в рублях накопленным итогом с даты регистрации первой потери;»;

абзац сорок пятый изложить в следующей редакции:

«источники получения возмещения (от страховой организации, иностранной страховой организации, входящих в банковскую группу, страховой организации, иностранной страховой организации, не входящих в банковскую группу, связанных с кредитной организацией (головной кредитной организацией банковской группы, участниками банковской группы) лиц в соответствии со статьей 64^1 Федерального закона № 86-ФЗ, контрагента, работников кредитной организации (головной кредитной организации банковской группы, участников банковской группы) и других третьих лиц);»;

в абзаце сорок шестом слово «(фактических)» исключить.

1.14. В пункте 6.7:

абзац первый после слова «валовых» дополнить словом «прямых», после слова «включаются» дополнить словом «прямые»;

в абзаце втором после слова «валовых» дополнить словом «прямых», слова «(за исключением событий операционного риска, связанных с реализацией кредитного риска)» исключить;

абзацы первый и пятый подпункта 6.7.1 после слова «валовых» дополнить словом «прямых»;

подпункт 6.7.2 после слова «идентификации» дополнить словом «прямых»;

в подпункте 6.7.3:

абзац первый после слова «валовые» дополнить словом «прямые»;

абзац пятый признать утратившим силу.

1.15. Пункт 6.9 после слов «всех видов операционного риска,» дополнить словами «в том числе событий риска нарушения непрерывности деятельности,».

1.16. В пункте 6.12:

абзац второй после слов «тип события операционного риска» дополнить словами «и (или) вид потерь»;

дополнить абзацем следующего содержания:

«Кредитная организация (головная кредитная организация банковской группы) регистрирует группу событий в базе событий как одно событие операционного риска с указанием количества событий операционного риска, включенных в группу событий.».

1.17. В пункте 6.13 слова «, другой бухгалтерской записи» заменить словами «по счетам расходов или убытков, другой бухгалтерской записи по счетам бухгалтерского учета, отражающих поступление возмещения,».

1.18. В пункте 6.14:

абзац первый после слова «каждой» дополнить словом «прямой»;

дополнить абзацем следующего содержания:

«Кредитная организация (головная кредитная организация банковской группы) в случае получения возмещения по косвенным потерям (включая страховые выплаты, направленные на возмещение убытков, связанных с нарушением операционной устойчивости кредитной организации (головной кредитной организации банковской группы) и (или) приостановкой основных и прочих процессов, определяемых кредитной организацией (головной кредитной организацией банковской группы) в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения, из-за реализации источников операционного риска) вправе учитывать полученные возмещения при определении величины косвенной потери расчетным методом как без отражения отдельной записи о возмещении в базе событий (производится перерасчет величины косвенной потери с указанием

информации о полученном возмещении), так и с отражением в базе событий отдельной записи о сумме полученного возмещения.».

1.19. Абзац четвертый пункта 6.15 дополнить словами «, иностранных страховых организаций».

1.20. В абзаце первом пункта 6.17 слово «(фактические)» исключить, дополнить предложениями следующего содержания: «Кредитная организация (головная кредитная организация банковской группы) в целях расчета суммы чистых потерь по событию операционного риска учитывает сумму возмещений, не превышающую сумму потерь в рублях. Кредитная организация (головная кредитная организация банковской группы) вправе не отражать поступившие возмещения в базе событий. В этом случае сумма чистых потерь от реализации события операционного риска в базе событий должна быть равна сумме валовых потерь от реализации данного события операционного риска.».

1.21. В пункте 6.18 слово «(фактические)» исключить, слово «возмещения» заменить словом «возмещений».

1.22. В абзаце третьем пункта 7.2 слово «связанных» заменить словом «связанные».

1.23. В абзаце первом пункта 7.3 слова «от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», зарегистрированным Министерством юстиции Российской Федерации 14 июня 2012 года № 24575, 1 июля 2013 года № 28930, 10 сентября 2014 года № 34017, 22 июня 2018 года № 51411 (далее – Положение Банка России № 382-П)» заменить словами «от 4 июня 2020 года № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении

переводов денежных средств», зарегистрированным Министерством юстиции Российской Федерации 23 сентября 2020 года № 59991 (далее – Положение Банка России № 719-П)», после слов «прямые и» дополнить словом «(или)».

1.24. Пункт 7.6 дополнить предложением следующего содержания: «В случае выявления событий риска информационной безопасности, связанных с не контролируемым кредитной организацией (головной кредитной организацией банковской группы) распространением сведений, составляющих банковскую тайну, кредитная организация (головная кредитная организация банковской группы) обеспечивает их регистрацию в базе событий, включающую описание указанных событий риска информационной безопасности в соответствии с пунктом 6.6 настоящего Положения.».

1.25. В пункте 7.7:

в абзаце пятом слова «, или его заместителю)» исключить;

абзацы шестой – восемнадцатый изложить в следующей редакции:

«выявление событий риска информационной безопасности, включая рассмотрение обращений клиентов, контрагентов, работников и третьих лиц, связанных с нарушением информационной безопасности, выявление и регистрацию инцидентов защиты информации, выявление фактов компрометации объектов информационной инфраструктуры;

обеспечение осведомленности кредитной организации (головной кредитной организации банковской группы) и участников технологических процессов об актуальных угрозах безопасности информации, обмен информацией о событиях риска информационной безопасности, в том числе об инцидентах защиты информации, и представление данных в Банк России в соответствии с требованиями пункта 8 Положения Банка России № 683-П;

организацию ресурсного (кадрового и финансового) обеспечения, включая установление требований к квалификации работников кредитной организации (головной кредитной организации банковской группы), в том

числе должностного лица (лица, его замещающего), ответственного за функционирование системы обеспечения информационной безопасности;

повышение осведомленности, обучение и развитие навыков работников кредитной организации (головной кредитной организации банковской группы) в области противодействия угрозам безопасности информации;

установление и реализацию программ контроля, в том числе программ аудита, включая независимую оценку соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в соответствии с требованиями пункта 9 Положения Банка России № 683-П;

проведение мониторинга риска информационной безопасности;

соответствие фактических значений контрольных показателей уровня риска информационной безопасности принятым в кредитной организации (головной кредитной организации банковской группы) значениям;

планирование, разработку, реализацию, контроль и совершенствование комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности, в том числе в соответствии с реализуемыми уровнями защиты информации в отношении объектов информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в соответствии с требованиями подпункта 3.1 пункта 3 Положения Банка России № 683-П;

обеспечение защиты от угроз безопасности информации, включая обеспечение защиты информации, управление риском информационной безопасности при передаче третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы) выполнения отдельных функций кредитной организации (головной кредитной организации

банковской группы) и (или) использовании внешних информационных систем в рамках реализации направлений деятельности, в том числе в разрезе составляющих их процессов, кредитной организации (головной кредитной организации банковской группы), управление риском несанкционированного доступа внутреннего нарушителя, являющегося работником кредитной организации (головной кредитной организации банковской группы) или третьим лицом, обладающими полномочиями по доступу к объектам информационной инфраструктуры кредитной организации (далее – внутренний нарушитель), предотвращение не контролируемого кредитной организацией (головной кредитной организацией банковской группы) распространения сведений, составляющих банковскую тайну, а также обеспечение операционной надежности;

порядок реагирования на выявленные события риска информационной безопасности, в том числе инциденты защиты информации, и восстановления деятельности кредитной организации (головной кредитной организации банковской группы) в случае реализации таких событий, включая порядок взаимодействия кредитной организации (головной кредитной организации банковской группы) с клиентами и третьими лицами, в том числе в случае получения уведомлений, связанных с осуществлением перевода денежных средств без согласия клиентов;

выполнение требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, в соответствии с пунктом 5 Положения Банка России № 683-П;

процессы применения прикладного программного обеспечения автоматизированных систем и приложений, соответствующих требованиям пункта 4 Положения Банка России № 683-П;

ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры

в соответствии с подпунктом 3.2 пункта 3 Положения Банка России № 683-П.».

1.26. В пункте 7.8:

абзац третий дополнить словами «и задачи управления риском информационной безопасности»;

абзац седьмой изложить в следующей редакции:

«требования к третьим лицам (внешним подрядчикам, контрагентам, участникам банковской группы), которым могут быть переданы функции кредитной организации (головной кредитной организации банковской группы) по обеспечению информационной безопасности, а также определение порядка взаимодействия и распределения ответственности между кредитной организацией (головной кредитной организацией банковской группы) и привлеченными ею третьими лицами.».

1.27. В подпункте 7.9.2 пункта 7.9:

абзац пятый признать утратившим силу;

в абзаце шестом слова «, а при его отсутствии – коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы)» исключить.

1.28. Пункт 7.10 изложить в следующей редакции:

«7.10. Служба информационной безопасности формирует сводные отчеты по рискам информационной безопасности, направляемые на рассмотрение должностному лицу, ответственному за обеспечение информационной безопасности, и коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы), в дополнение к отчетам, формируемым подразделением, ответственным за организацию управления операционным риском в соответствии с пунктом 4.2 настоящего Положения.

Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах порядок и сроки представления данных отчетов.».

1.29. В пункте 8.3:

абзац третий дополнить словами «, не участвующее в совершении операций, сделок, организации бухгалтерского и управленческого учета, обеспечении функционирования системы обеспечения информационной безопасности, с прямым подчинением лицу, осуществляющему функции единоличного исполнительного органа кредитной организации (головной кредитной организации банковской группы)»;

абзац четвертый признать утратившим силу.

1.30. Пункт 8.5 изложить в следующей редакции:

«8.5. Кредитная организация (головная кредитная организация банковской группы) описывает во внутренних документах архитектуру информационных систем и состав ее элементов, в том числе с учетом оценки влияния на них третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы):

информационных систем кредитной организации (головной кредитной организации банковской группы) с соотнесением их элементов с процессами в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения, выполнение которых они обеспечивают;

структуры информационного обмена между элементами информационных систем, используемых при обеспечении процессов кредитной организации (головной кредитной организации банковской группы);

информационных систем третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы) и их элементов, обеспечивающих процессы кредитной организации (головной кредитной организации банковской группы), и структуры информационного обмена между их элементами и элементами других информационных систем кредитной организации (головной кредитной организации банковской группы). Кредитная организация (головная кредитная организация банковской группы) в случае отсутствия информации об информационных

системах третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы) документирует причины и учитывает отсутствие указанной информации при оценке уровня риска информационных систем, в том числе в соответствии с абзацами седьмым и восьмым подпункта 8.7.2 пункта 8.7 настоящего Положения;

подразделений и работников подразделений кредитной организации (головной кредитной организации банковской группы) и (или) третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы), являющихся пользователями и (или) обеспечивающих функционирование информационных систем.».

1.31. В пункте 8.7:

абзац первый после слова «процессов» дополнить словами «и операционную устойчивость»;

в подпункте 8.7.1:

в абзаце третьем слова «внешних поставщиков услуг и информации (провайдеров, операторов связи или других контрагентов)» заменить словами «третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы)»;

в абзаце четвертом слова «и провайдеров» заменить словами «(внешних подрядчиков, контрагентов, участников банковской группы)»;

абзац седьмой подпункта 8.7.2 изложить в следующей редакции:

«закупке услуг и информации в случае необходимости привлечения третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы), в том числе порядку их выбора, определения их ответственности и правил их взаимодействия;».

1.32. В абзаце третьем подпункта 9.1.1 пункта 9.1 слово «семнадцатого» заменить словом «девятнадцатого».

1.33. В подпункте 9.2.1 пункта 9.2:

абзац третий изложить в следующей редакции:

«требования абзацев первого – третьего, четвертого (в части анализа динамики КИР по критически важным процессам) подпункта 2.1.1, подпункта 2.1.2 (банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, с учетом порога регистрации фиксирует в базе событий события операционного риска с прямыми и (или) косвенными потерями, а также потерями, указанными в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения), подпункта 2.1.3, абзацев первого, третьего – пятого подпункта 2.1.4, абзацев первого, второго, четвертого – тринадцатого, шестнадцатого – девятнадцатого подпункта 2.1.5, подпунктов 2.1.6 и 2.1.7 пункта 2.1, пунктов 2.2–2.5 настоящего Положения;»;

абзац четвертый после цифр «4.2,» дополнить словами «подпунктов 4.3.3 и 4.3.4 пункта 4.3, пунктов».

1.34. В абзаце третьем подпункта 9.3.1 пункта 9.3 слова «абзацев первого – третьего подпункта 2.1.4» заменить словами «абзацев первого, третьего и четвертого подпункта 2.1.4, абзацев первого, четвертого (в части моделирования угроз), девятнадцатого подпункта 2.1.5».

1.35. В абзаце пятом пункта 9.4 слова «абзацев первого – шестого» заменить словами «абзацев первого – четвертого, шестого».

1.36. В приложении 1:

в пункте 1:

в подпункте 1.1.1:

в абзаце втором слово «валовых» заменить словом «чистых», после слов «за вычетом» дополнить словами «чистых прямых»;

абзац третий после слов «за вычетом» дополнить словами «валовых прямых»;

абзац четвертый изложить в следующей редакции:

«отношение общей суммы чистых прямых потерь (включая чистые прямые потери от реализации событий риска информационной

безопасности), понесенных кредитной организацией за год, к показателю объема операционного риска в виде показателя Д, рассчитанного в соответствии с пунктом 3 Положения Банка России № 652-П на последнюю отчетную дату для кредитных организаций, применяющих для расчета размера операционного риска Положение Банка России № 652-П, либо в виде показателя бизнес-индикатора, рассчитанного в соответствии с пунктом 2.2 Положения Банка России № 744-П на последнюю расчетную дату для кредитных организаций, применяющих для расчета размера операционного риска Положение Банка России № 744-П (далее – показатель объема операционного риска);»;

абзац пятый после слов «за вычетом» дополнить словами «валовых прямых»;

в абзаце шестом слово «(фактических)» исключить, после слов «за вычетом» дополнить словами «чистых прямых»;

абзац седьмой изложить в следующей редакции:

«доля выявленных (по количеству) в ходе оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, внешним экспертом или Банком России, событий операционного риска с валовыми прямыми потерями, превышающими порог регистрации, определяемый в соответствии с пунктом 6.5 настоящего Положения, которые кредитная организация не отразила в базе событий, по отношению ко всем зарегистрированным в базе событий событиям операционного риска с валовыми прямыми потерями, превышающими порог регистрации, за годовой период, к которому относится проверяемый период (контрольное значение должно быть не больше 5 процентов, сигнальное значение – не больше 3 процентов);»;

в абзаце восьмом слова «(за исключением потерь от реализации событий кредитного риска, связанных с реализацией операционного риска)» исключить;

абзац девятый после слов «прямых и» дополнить словами «сумм величин», после слов «за вычетом» дополнить словами «суммы валовых прямых и сумм величин косвенных»;

абзац десятый изложить в следующей редакции:

«отношение суммы чистых прямых и сумм величин косвенных потерь от реализации событий операционного риска, определяемых расчетным образом, за вычетом суммы чистых прямых и сумм величин косвенных потерь от реализации событий риска информационной безопасности, к общему капиталу (собственным средствам) кредитной организации на последнюю отчетную дату года;»;

в подпункте 1.2.1:

в абзаце втором слово «валовых» заменить словом «чистых»;

в абзаце четвертом слово «(фактических)» исключить;

абзац пятый после слова «потерь» дополнить словами «от реализации событий риска информационной безопасности», после слов «общей сумме» дополнить словами «осуществленных кредитной организацией»;

абзац седьмой изложить в следующей редакции:

«отношение суммы денежных средств, по которой получены уведомления, связанные с осуществлением перевода денежных средств без согласия клиента, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме переводов денежных средств за этот же период (контрольное значение должно быть не более 0,005 процента, сигнальное значение – не более 0,002 процента);»;

в абзаце восьмом слова «по отношению» заменить словами «, которые кредитная организация не отразила в базе событий, по отношению», слова «сообщила в своих отчетах в Банк России, направляемых» заменить словами «проинформировала Банк России»;

в абзаце девятом слова «не сообщила в своих отчетах в Банк России, направляемых» заменить словами «не проинформировала Банк России»,

слова «сообщила в своих отчетах в Банк России, направляемых в соответствии с пунктом 8 Положения Банка России № 683-П» заменить словами «проинформировала Банк России в соответствии с пунктом 8 Положения Банка России № 683-П, за годовой период, к которому относится проверяемый период»;

в абзаце десятом после слов «прямых и» дополнить словами «сумм величин», слова «методов, применяемых в международной практике (далее – продвинутый подход)» заменить словами «продвинутого подхода»;

в абзаце одиннадцатом слова «(фактических) прямых и» заменить словами «прямых и сумм величин»;

абзац двенадцатый изложить в следующей редакции:

«отношение суммы валовых прямых и сумм величин косвенных потерь, понесенных кредитной организацией при выполнении кредитной организацией функций оператора платежной системы или оператора услуг платежной инфраструктуры, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме операций по переводу денежных средств через платежные системы, где кредитная организация выполняет функции оператора платежной системы, за этот же период (в случае, если кредитная организация применяет продвинутый подход к расчету объема капитала, выделяемого на покрытие потерь от реализации операционного риска);»;

абзац тринадцатый после слов «прямых и» дополнить словами «сумм величин»;

в абзаце четырнадцатом после слов «прямых и» дополнить словами «сумм величин», слова «и снятия» заменить словом «(снятия)»;

дополнить абзацами следующего содержания:

«отношение количества операций по переводу денежных средств, соответствующих признакам осуществления перевода денежных средств без согласия клиента – физического лица, размещенным на официальном сайте

Банка России в информационно-телекоммуникационной сети «Интернет» (далее соответственно – сеть «Интернет», операции, соответствующие признакам осуществления перевода денежных средств без согласия клиента – физического лица), в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2018, № 27, ст. 3950) приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общему количеству операций по переводу денежных средств за этот же период;

отношение суммы денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме денежных средств по операциям по переводу денежных средств за этот же период;

отношение количества операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств и по которым

получены подтверждения клиентов – физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены от клиентов – физических лиц подтверждения возобновления исполнения распоряжений в соответствии с частью 5^3 статьи 8 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2018, № 27, ст. 3950), за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к количеству операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за этот же период;

отношение суммы денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств и по которым получены подтверждения клиентов – физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены от клиентов – физических лиц подтверждения возобновления исполнения распоряжений в соответствии с частью 5^3 статьи 8 Федерального закона № 161-ФЗ, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств по операциям, соответствующим признакам

осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за этот же период;

отношение количества операций по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ и по которым получены уведомления от клиентов – физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872), за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к количеству операций по переводу денежных средств без согласия клиента – физического лица за этот же период;

отношение суммы денежных средств по операциям по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ и по которым получены уведомления от клиентов – физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона № 161-ФЗ, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств по операциям по переводу денежных средств без согласия клиента – физического лица за этот же период;

отношение суммы денежных средств, возмещенной (возвращенной) клиентам, по которой получены уведомления от клиентов об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона № 161-ФЗ, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств, в отношении которой получены такие уведомления, за этот же период;

оценка соответствия уровню защиты информации в отношении процесса 1 «Обеспечение защиты информации при управлении доступом», определенного пунктом 7.2 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст (М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017), согласно методике оценки соответствия защиты информации, определенной национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2-2018) (контрольное значение должно быть не менее 0,85, сигнальное значение – не менее 0,9);

оценка соответствия уровню защиты информации в отношении процесса 5 «Предотвращение утечек информации», определенного пунктом 7.6 ГОСТ Р 57580.1-2017, согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2-2018 (контрольное значение должно быть не менее 0,85, сигнальное значение – не менее 0,9);

оценка выполнения установленных Положением Банка России № 683-П, Положением Банка России № 719-П, Положением Банка России от 23 декабря 2020 года № 747-П «О требованиях к защите информации в платежной системе Банка России», зарегистрированным Министерством юстиции Российской Федерации 3 февраля 2021 года № 62365, требований к обеспечению защиты информации, применяемых в отношении объектов информационной инфраструктуры, проводимая согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2-2018.

При расчете количественного контрольного показателя уровня риска информационной безопасности, указанного в абзаце девятнадцатом настоящего подпункта, кредитная организация (головная кредитная организация банковского группы) определяет количество операций по переводу денежных средств без согласия клиента – физического лица как сумму количества операций по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ и по которым получены уведомления от клиентов – физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона № 161-ФЗ, и количества операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за исключением случаев, когда получены подтверждения клиентов – физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены от клиентов – физических лиц подтверждения возобновления

исполнения распоряжений в соответствии с частью 5^3 статьи 8 Федерального закона № 161-ФЗ.

При расчете количественного контрольного показателя уровня риска информационной безопасности, указанного в абзаце двадцатом настоящего подпункта, кредитная организация (головная кредитная организация банковского группы) определяет сумму денежных средств по операциям по переводу денежных средств без согласия клиента – физического лица как сумму денежных средств по операциям по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ и по которым получены уведомления от клиентов – физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона № 161-ФЗ, и денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента – физического лица, в отношении которых кредитная организация в соответствии с частью 5 статьи 8 Федерального закона № 161-ФЗ не приняла к исполнению и (или) в соответствии с частью 5^1 статьи 8 Федерального закона № 161-ФЗ приостановила исполнение распоряжений о совершении операций по переводу денежных средств, за исключением случаев, когда получены подтверждения клиентов – физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены от клиентов – физических лиц подтверждения возобновления исполнения распоряжений в соответствии с частью 5^3 статьи 8 Федерального закона № 161-ФЗ.»;

подпункт 1.2.2 изложить в следующей редакции:

«1.2.2. Качественные контрольные показатели риска информационной безопасности, к которым относятся качественные оценки по четырехуровневой системе («хорошо», «удовлетворительно», «сомнительно»,

«неудовлетворительно»), по направлению «оценка эффективности функционирования системы управления риском информационной безопасности, проведенная уполномоченным подразделением и (или) внешним экспертом (специализированной организацией или квалифицированным внешним экспертом) по решению совета директоров (наблюдательного совета) кредитной организации».».

1.37. В приложении 2:

абзац второй пункта 1 изложить в следующей редакции:

«регуляторный подход, основанный на расчете размера операционного риска в соответствии с пунктом 2 Положения Банка России № 652-П в случае, если кредитная организация применяет для целей расчета размера операционного риска Положение Банка России № 652-П, либо в соответствии с пунктом 1.2 Положения Банка России № 744-П в случае, если кредитная организация применяет для целей расчета размера операционного риска Положение Банка России № 744-П, и прогнозных сценариев среднегодовых потерь от реализации событий операционного риска, изложенный в пункте 4 настоящего приложения (далее – регуляторный подход);»;

в пункте 3:

абзац восьмой изложить в следующей редакции:

«ОР – целевое (прогнозное) значение на планируемый период размера операционного риска, определяемого в соответствии с пунктом 2 Положения Банка России № 652-П в случае, если кредитная организация применяет для целей расчета размера операционного риска Положение Банка России № 652-П, либо в соответствии с пунктом 1.2 Положения Банка России № 744-П в случае, если кредитная организация применяет для целей расчета размера операционного риска Положение Банка России № 744-П;»;

в абзаце десятом слова «на базе сценарного анализа в части возможного превышения фактической величины прямых (совокупных)

потерь над контрольным значением контрольного показателя – лимита прямых (совокупных) годовых потерь от реализации событий риска информационной безопасности, установленного в соответствии с подпунктом 1.2.1 пункта 1 приложения 1 к настоящему Положению» заменить словами «с использованием анализа возможного превышения фактической величины чистых прямых потерь над контрольным значением контрольного показателя – общей суммой чистых прямых годовых потерь от реализации событий риска информационной безопасности, установленного в соответствии с абзацем вторым подпункта 1.2.1 пункта 1 приложения 1 к настоящему Положению»;

в абзаце одиннадцатом слова «на базе сценарного анализа в части возможного превышения фактической величины прямых (совокупных) потерь над контрольным значением контрольного показателя – лимита прямых (совокупных) годовых потерь от реализации событий операционного риска за вычетом лимита прямых потерь от реализации событий риска информационной безопасности, установленного в соответствии с подпунктом 1.1.1 пункта 1 приложения 1 к настоящему Положению» заменить словами «с использованием анализа возможного превышения фактической величины чистых прямых потерь над контрольным значением контрольного показателя – общей суммой чистых прямых годовых потерь от реализации событий операционного риска за вычетом чистых прямых потерь от реализации событий риска информационной безопасности, установленного в соответствии с абзацем вторым подпункта 1.1.1 пункта 1 приложения 1 к настоящему Положению»;

в подпункте 4.3 пункта 4 слова «сценарного анализа» заменить словами «результатов качественной оценки уровня операционного риска, проведенной в соответствии с планом проведения качественной оценки, за последний календарный год».

1.38. В приложении 4:

в подпункте 4.5 пункта 4 слова «контрагентов (поставщиков услуг)» заменить словами «третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы)»;

подпункт 7.5 пункта 7 изложить в следующей редакции:

«7.5. недостатки работы с третьими лицами (внешними подрядчиками, контрагентами, участниками банковской группы), выбора третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы). К данному типу событий операционного риска относятся события операционного риска, связанные с потерями кредитной организации, возникшими в результате работы третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы), появлением зависимости процессов от третьих лиц (внешних подрядчиков, контрагентов, участников банковской группы);».

1.39. В приложении 5:

в абзаце четвертом подпункта 1.1 пункта 1 слова «информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»)» заменить словами «сети «Интернет»;

в пункте 2:

в подпункте 2.2 слова «персонала кредитной организации или третьих лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры кредитной организации» заменить словами «внутреннего нарушителя»;

абзац первый подпункта 2.6 после слова «информации» дополнить словами «(информационных угроз)».

2. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 11 февраля 2022 года № ПСД-2) вступает в силу с 1 октября 2022 года, за исключением подпункта 1.36 пункта 1 настоящего Указания.

Подпункт 1.36 пункта 1 настоящего Указания вступает в силу с 1 января 2023 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина